



# **OSD Systems Engineering Status and Goals**

**Stephen Welby**

**Deputy Assistant Secretary of Defense  
for Systems Engineering**

**AIA Technical Operations Council (TOC)  
May 1, 2013**



# Better Buying Power 2.0

## A Guide to Help You Think



### Achieve Affordable Programs

- Mandate affordability as a requirement
- Institute a system of investment planning to derive affordability caps
- Enforce affordability caps

### Control Costs Throughout the Product Lifecycle

- Implement “should cost” based management
- Eliminate redundancy within warfighter portfolios
- Institute a system to measure the cost performance of programs and institutions and to assess the effectiveness of acquisition policies
- Build stronger partnerships with the requirements community to control costs
- Increase the incorporation of defense exportability features in initial designs

### Incentivize Productivity & Innovation in Industry and Government

- Align profitability more tightly with Department goals
- Employ appropriate contract types
- Increase use of Fixed Price Incentive contracts in Low Rate Initial Production
- Better define value in “best value” competitions
- Only use LPTA when able to clearly define Technical Acceptability
- Institute a superior supplier incentive program
- Increase effective use of Performance-based Logistics
- Reduce backlog of DCAA Audits without compromising effectiveness
- Expand programs to leverage industry’s IR&D

### Reduce Unproductive Processes and Bureaucracy

- Reduce frequency of higher headquarters level reviews
- Re-emphasize AE, PEO and PM responsibility, authority, and accountability
- Reduce cycle times while ensuring sound investment decisions

### Promote Effective Competition

- Emphasize competition strategies and creating and maintaining competitive environments
- Enforce open system architectures and effectively manage technical data rights
- Increase small business roles and opportunities
- Use the Technology Development phase for true risk reduction

### Improve Tradecraft in Acquisition of Services

- Assign senior managers for acquisition of services
- Adopt uniform services market segmentation
- Improve requirements definition/prevent requirements creep
- Increase small business participation, including through more effective use of market research
- Strengthen contract management outside the normal acquisition chain – installations, etc.
- Expand use of requirements review boards and tripwires

### Improve the Professionalism of the Total Acquisition Workforce

- Establish higher standards for key leadership positions
- Establish stronger professional qualification requirements for all acquisition specialties
- Increase the recognition of excellence in acquisition management
- Continue to increase the cost consciousness of the acquisition workforce – change the culture

***For additional information on Better Buying Power 2.0: <http://bbp.dau.mil/>***



# DASD, Systems Engineering Mission



## **Systems Engineering focuses on engineering excellence – the creative application of scientific principles:**

- To design, develop, construct and operate complex systems
- To forecast their behavior under specific operating conditions
- To deliver their intended function while addressing economic efficiency, environmental stewardship and safety of life and property

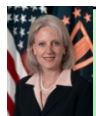
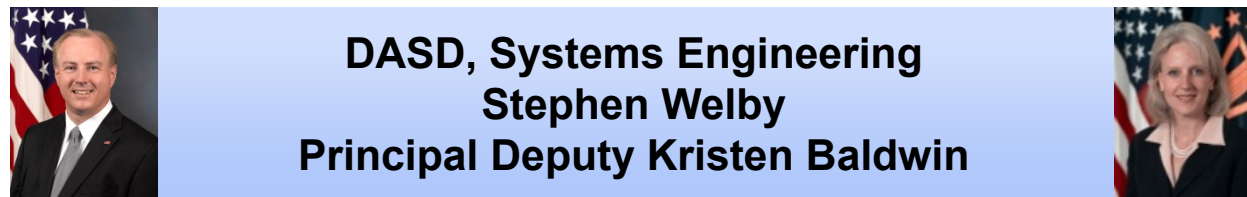
***DASD(SE) Mission: Develop and grow the Systems Engineering capability of the Department of Defense – through engineering policy, continuous engagement with component Systems Engineering organizations and through substantive technical engagement throughout the acquisition life cycle with major and selected acquisition programs.***

**A Robust Systems Engineering Capability Across the Department Requires Attention to Policy, People and Practice**

- ***US Department of Defense is the World's Largest Engineering Organization***
- ***Over 99,000 Uniformed and Civilian Engineers***
- ***Over 39,000 in the Systems Engineering (SPRDE) Acquisition Workforce***



# DASD, Systems Engineering



## **Systems Analysis** **Kristen Baldwin (Acting)**

*Addressing Emerging Challenges on the Frontiers of Systems Engineering*

**Analysis of Complex Systems/Systems of Systems**

**Program Protection/Acquisition Cyber Security**

**University, FFRDC and Industry Engineering and Research**

**Modeling and Simulation**



## **Major Program Support** **James Thompson**

*Supporting USD(AT&L) Decisions with Independent Engineering Expertise*

**Engineering Assessment / Mentoring of Major Defense Programs**

**Program Support Reviews**

**OIPT / DAB / ITAB Support**

**Systems Engineering Plans**

**Systemic Root Cause Analysis**



## **Mission Assurance** **Nicholas Torelli**

*Leading Systems Engineering Practice in DoD and Industry*

**Systems Engineering Policy & Guidance**

**Development Planning/Early SE**

**Specialty Engineering (System Safety, Reliability and Maintainability Engineering, Quality, Manufacturing, Producibility, Human Systems Integration)**

**Counterfeit Prevention**

**Technical Workforce Development**

**Standardization**

**Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs**



# SE Annual Report to Congress



**DEPARTMENT OF DEFENSE  
Systems Engineering  
FY 2012 Annual Report**



MARCH 2013

Preparation of this report cost the Department of Defense a total of approximately \$----- in FY 2012-2013.  
Generated on 2013Mar----- 1409 RefID: 9-37B8F44  
WHS Report Control Symbol DD-AT&L(A)2258

**Deputy Assistant Secretary of Defense for Systems Engineering**

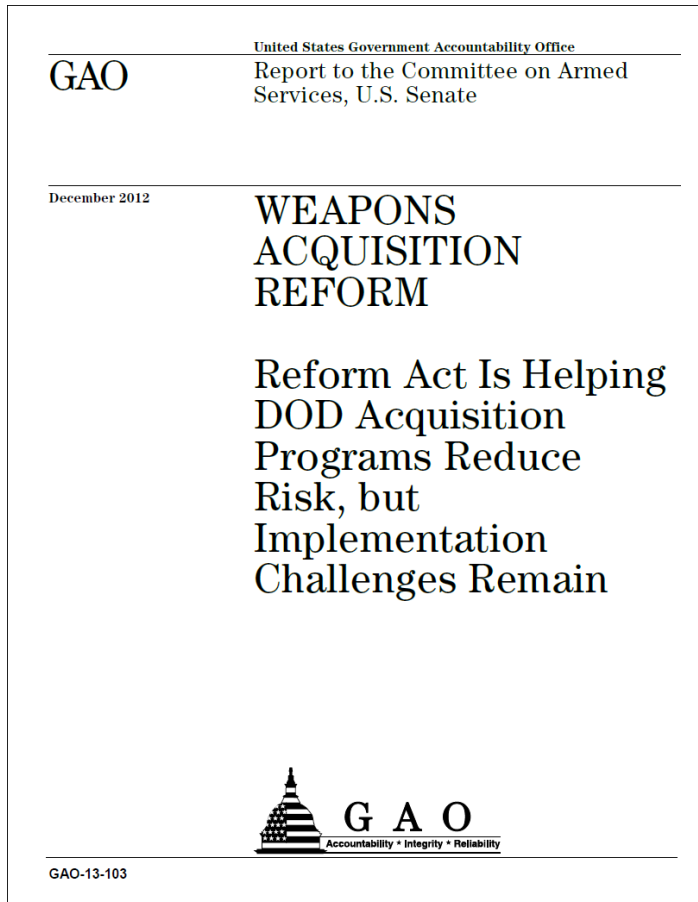
Washington, D.C.

- **FY 2012 SE Annual Report delivered to Congress**
- **Detailed review of DASD(SE) accomplishments in FY12**
- **Review of Service progress and plans implementing key pieces of WSARA to improve SE capabilities**
- **Detailed program by program assessments for 40+ MDAPs**

<http://www.acq.osd.mil/se/docs/SE-FY12-AnnualReport-28March2013-Final.pdf>



# GAO Report 13-103 Findings DASD(SE) Performance



- Completed the development of systems engineering and development planning policy, guidance and performance measures
- Regularly completing MDAP document review and approval and program monitoring and assessments
- Led working group efforts to support Service initiatives to address systemic reliability issues in UAS and rotary wing portfolios
- Led workforce development initiatives to attract and retain a qualified SE workforce and support KLP implementation
- Positively impacted the requirements development and technical and reliability planning for:
  - Joint Lightweight Tactical Vehicle
  - Ground Combat Vehicle
  - Joint Strike Fighter
  - Remote Mine-hunting System
  - Gray Eagle and Global Hawk

<http://www.gao.gov/products/GAO-13-103>





# Top Level FY13 DASD(SE) Goals



- **Continue excellence in SE support to programs and acquisition decisions**
- **Improve consistent program protection plan (PPP) engagement with programs resulting in successful vulnerability mitigation strategies**
- **Advocate for and ensure SE workforce capacity and capability**
- **Provide depth to acquisition policy and processes with SE guidance, practices, and continuous learning opportunities**
- **Advance the state of engineering to meet challenges and enable DoD goals**
- **Maintain quality of technical insight in resource constrained environment**



# FY13 DASD(SE) Objectives



- **Engineering Program Support**
  - Provide engineering assessment / mentoring of major defense acquisition programs
  - Support acquisition leadership with independent engineering analysis and advice
  - Support, review and approve Systems Engineering Plans
  - Engage with programs in support of preliminary design review/critical design reviews (PDR/CDR) assessments
  - Institutionalize software assessment support capability
  - Develop an update to the DoD Risk Management Guide to implement a risk management approach for PMs
  - Program data analysis and benchmarking
- **Engineering Workforce**
  - Publish Human Capital Strategic Plan content for Engineering Non-Construction, SPRDE and PQM career fields
  - Oversee implementation of Lead Systems Engineer Key Leadership Position (KLP)





# FY13 DASD(SE) Objectives



- **Engineering Policy and Guidance**

- Promulgate revised engineering guidance in DoDI 5000 and publish an update to the Defense Acquisition Guidebook Chapter 4 – Systems Engineering
- Oversee Value Engineering activities in support of Better Buying Power (BBP) 2.0
- Publish Open Systems Architecture guidance in support of BBP 2.0
- Finalize DAES reporting guidance for Reliability and Maintainability Engineering
- Publish guidance on risk-based counterfeit prevention, in coordination with L&MR and DPAP, in support of FY12 NDAA Section 818 and FY13 NDAA Section 833

- **Technical Standards**

- Oversee DoD update to 5 (non-government) technical standards:  
1) Systems Engineering, 2) Technical Reviews/Audits, 3) Configuration Management, 4) Logistics Support, and 5) Manufacturing Management
- Oversee Government Industry Data Exchange Program (GIDEP) requirements update and implementation in support of FY12 NDAA Section 818 Counterfeit Prevention activities



# FY13 DASD(SE) Objectives



- **Program Protection**
  - Conduct Anti-Tamper study to support exportability BBP 2.0 initiative
  - Update Software Assurance policy/guidance in compliance with FY13 NDAA Section 933
  - Implement AT&L strategy for Defense Industrial Board (DIB) Cyber Security/Safeguarding Unclassified information, and Supply Chain Risk Management in support of NDAA Section 941
  - Support acquisition program implementation of trusted microelectronics strategies in accordance with DoDI 5200.44 requirements for trusted ASICs and FPGA strategy



# Defense Acquisition Guidebook (DAG) Chapter 4 Systems Engineering Update



- **Improve guidance to fully reflect current policy and DASD(SE) initiatives:**
  - Joint Capabilities Integration and Development System (JCIDS) (Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01H)
  - Process changes as a result of Better Buying Power
  - Systemic root cause analyses findings
  - Department-wide best practice; avoiding Service and domain-specific implementations
- **Improve currency, consistency, usability, and readability—less theory, more utility**
- **Emphasize the role of Systems Engineering in providing balanced solutions (managing cost, schedule and risk) that deliver needed capability to the war fighter**
- **Make Chapter 4 an effective tool for the Program Manager and the Systems Engineering Practitioner**

<https://acc.dau.mil>



# Proposed DoD 5000.02 Update



- **Decrease emphasis on “rules” and increase emphasis on process intent and thoughtful program planning**
- **Provide program structures and procedures tailored to the dominant characteristics of the product being acquired and to unique program circumstances, e.g., risk and urgency**
- **Added key decision points between Milestone A and Milestone B**
- **Institutionalize changes to statute and policy since the last issuance of DoD Instruction 5000.02**

Department of Defense Instruction (DoDI) 5000.02 Operation of the Defense Acquisition System



# Program Protection Integrated in Policy



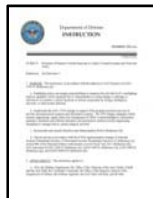
## DoDI 5000.02 Operation of the Defense Acquisition System

- Regulatory Requirement for Program Protection Plan at Milestones A, B, C and FRP/FDD
- References DoDI 5200.39



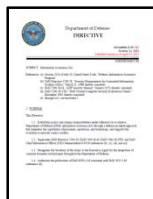
## DoDI 5200.39 Critical Program Information (CPI) Protection Within the DoD

- Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
- Expands definition of CPI to include degradation of mission effectiveness



## DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks

- Establishes policy and responsibilities to minimize the risk that warfighting capability will be impaired due to vulnerabilities in system design or subversion of mission critical functions or components



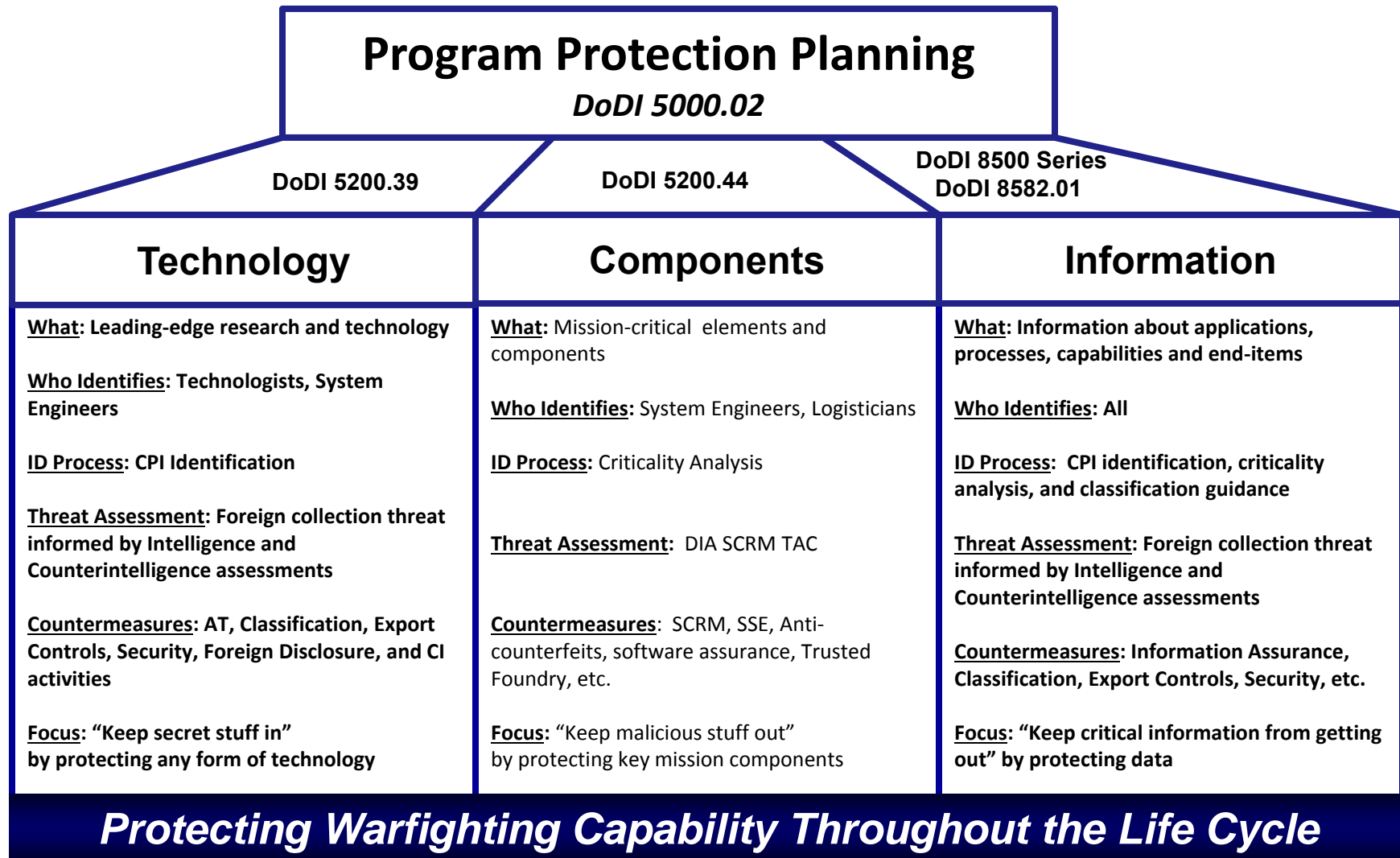
## DoDI 8500.01E Information Assurance

- Establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare

DoD Issuances Website: <http://www.dtic.mil/whs/directives/corres/ins1.html>



# What Are We Protecting?







# DoDI 5200.44

## Trusted Systems and Networks



### Department of Defense INSTRUCTION

NUMBER 5200.44  
November 5, 2012

DoD CIO/USD(AT&L)

**SUBJECT:** Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)

**References:** See Enclosure 1

1. **PURPOSE.** This Instruction, in accordance with the authorities in DoD Directive (DoDD) 5134.01 (Reference (a)) and DoDD 5144.1 (Reference (b)):

a. Establishes policy and assigns responsibilities to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design or sabotage or subversion of a system's mission critical functions or critical components, as defined in this Instruction, by foreign intelligence, terrorists, or other hostile elements.

b. Implements the DoD's TSN strategy, described in the Report on Trusted Defense Systems (Reference (c)) as the Strategy for Systems Assurance and Trustworthiness, through Program Protection and information assurance (IA) implementation to provide uncompromised weapons and information systems. The TSN strategy integrates robust systems engineering, supply chain risk management (SCRM), security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines to manage risks to system integrity and trust.

c. Incorporates and cancels Directive-Type Memorandum 09-016 (Reference (d)).

d. Directs actions in accordance with the SCRM implementation strategy of National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (e)), section 806 of Public Law 111-383 (Reference (f)), DoD Instruction (DoDI) 5200.39 (Reference (g)), DoDD 5000.01 (Reference (h)), DoDI 5000.02 (Reference (i)), DoDD 8500.01E (Reference (j)), and Committee on National Security Systems Directive No. 505 (Reference (k)).

2. **APPLICABILITY.** This Instruction applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

- Implements the DoD's Trusted Systems and Networks (TSN) strategy
- Manage risk of mission-critical function and component compromise throughout lifecycle of key systems by utilizing
  - Criticality Analysis as the systems engineering process for risk identification
  - Countermeasures: Supply chain risk management, software assurance, secure design patterns
  - Intelligence analysis to inform program management
- Codify trusted supplier requirement for DoD-unique application-specific integrated circuits (ASICs)
- Document planning and accomplishments in program protection and information assurance activities



# FY13 NDAA Section 941



## SEC. 941. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) **PROCEDURES FOR REPORTING PENETRATIONS.**—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) **NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.**—

(1) **CRITERIA.**—The Secretary of Defense shall designate a senior official to, in consultation with the officials specified in paragraph (2), establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

(2) **OFFICIALS.**—The officials specified in this subsection are the following:

- (A) The Under Secretary of Defense for Policy.
- (B) The Under Secretary of Defense for Acquisition, Technology, and Logistics.
- (C) The Under Secretary of Defense for Intelligence.
- (D) The Chief Information Officer of the Department of Defense.

(E) The Commander of the United States Cyber Command.

(c) **PROCEDURE REQUIREMENTS.**—

(1) **RAPID REPORTING.**—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following: (A) A description of the technique or method used

in such penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration. (C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

tion.

## FY13 NDAA SEC. 941: REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS

- “The Secretary of Defense shall establish procedures that require each cleared defense contractor to report ... when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.”

NDAA: National Defense Authorization Act <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf>



# Defense Industrial Base (DIB) Cyber Security



*“The private sector, government, military, our allies - all share the same global infrastructure and we all share the responsibility to protect it.”*

Secretary of Defense Leon E. Panetta  
October 11, 2012

## **DoD efforts to advance cyber security in the DIB include:**

- DIB Cyber Security/Information Assurance (CS/IA) Program, and its optional enhanced component the DIB Enhanced Cybersecurity Services (<http://dibnet.dod.mil>)
- Standards development in collaboration with Industry
- Reinforcing protection of technical information in acquisition activities



# System Security Community Activities




- **NDIA “Guidebook for System Assurance”, Version 1.0, 2008**
  - Process/technology guidance to increase the level of system assurance through a planned, systematic set of multi-disciplinary activities
  - <http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf>
- **ISO/IEC 15026 – System and Software Engineering – Systems and Software Assurance**
  - Establishes common assurance concepts, vocabulary, integrity levels and life cycle activities
- **ISO/IEC 27036 – IT Security Techniques – Supplier Relationships**
  - Establishes techniques between acquirer and supplier for supply chain risk management
- **International Council on Systems Engineering (INCOSE) Handbook**
  - Working group to develop security engineering updates to INCOSE SE Handbook
- **NIST - System Security Engineering (SSE) 800-160 Special Pub (In Development)**
  - Aligns SSE with ISO/IEC15288 terminology, incorporates DoD best practices
  - DoD Appendix targets DoD community, includes Systems Engineering Technical Review (SETR) criteria
- **The Open Group (TOG)**
  - The Open Trusted Technology Provider Framework (O-TTPF) - open standard that codifies best practices across the entire lifecycle (targeted against counterfeit HW & malicious SW)
  - <http://www.opengroup.org/ogttf/>



# Data Vulnerability Tiger Team



  
ACQUISITION,  
TECHNOLOGY  
AND LOGISTICS

THE UNDER SECRETARY OF DEFENSE  
3010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3010

FEB 07 2013

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR POLICY  
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE  
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER  
SERVICE ACQUISITION EXECUTIVES  
COMMANDER, UNITED STATES CYBER COMMAND


SUBJECT: Data Vulnerability Tiger Team

The Department of Defense (DoD) faces increasing challenges in adequately protecting sensitive UNCLASSIFIED information, and in particular is challenged in preventing the loss of sensitive weapon system technical data from UNCLASSIFIED computer networks, including networks and databases maintained by DoD contractors.

I am establishing a Data Vulnerability Tiger Team to review the Department's progress to date in protecting UNCLASSIFIED technical data and to identify further actions that may be taken to better safeguard sensitive technical data across the weapon system life cycle.

Mr. Alan F. Estevez, Assistant Secretary of Defense for Logistics and Materiel Readiness, will chair the Tiger Team. Mr. Estevez will host a Tiger Team kickoff meeting within 2 weeks.

I request each of your organizations identify a representative to participate on this Tiger Team. The Tiger Team will deliver initial findings and recommendations to me within 60 days. Please provide the name of your representative to Ms. Kristen Baldwin, Principal Deputy, DASD(SE), at [Kristen.Baldwin@osd.mil](mailto:Kristen.Baldwin@osd.mil).

  
Frank Kendall

cc:  
ASD(A)  
Director, DPAP  
Director, DCMA  
Director, MIBP  
DASD(C3&Cyber)  
DASD(S&TS)  
DASD(SIO)

- **USD(AT&L) Memorandum, February 7, 2013**
  - Established the Data Vulnerability Tiger Team
  - 60-day schedule
  - Review progress in protecting unclassified technical data
  - Identify further actions to take
- **Tiger Team actions**
  - Identify Focus Teams
  - Focus Teams will analyze gaps and recommend actions
  - Consolidate recommendations for USD(AT&L)





# FY13 NDAA Section 933



## SEC. 941. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCEDURES FOR REPORTING PENETRATIONS.—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.—

(1) CRITERIA.—The Secretary of Defense shall designate a senior official to, in consultation with the officials specified in paragraph (2), establish criteria for covered networks to be subject to the procedures for reporting system penetrations under subsection (a).

(2) OFFICIALS.—The officials specified in this subsection are the following:

- (A) The Under Secretary of Defense for Policy.
- (B) The Under Secretary of Defense for Acquisition, Technology, and Logistics.
- (C) The Under Secretary of Defense for Intelligence.
- (D) The Chief Information Officer of the Department of Defense.
- (E) The Commander of the United States Cyber Command.

(c) PROCEDURE REQUIREMENTS.—

(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following: (A) A description of the technique or method used in such penetration.

(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration. (C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

## FY13 NDAA SEC. 933: IMPROVEMENTS IN ASSURANCE OF COMPUTER SOFTWARE PROCURED BY THE DEPARTMENT OF DEFENSE

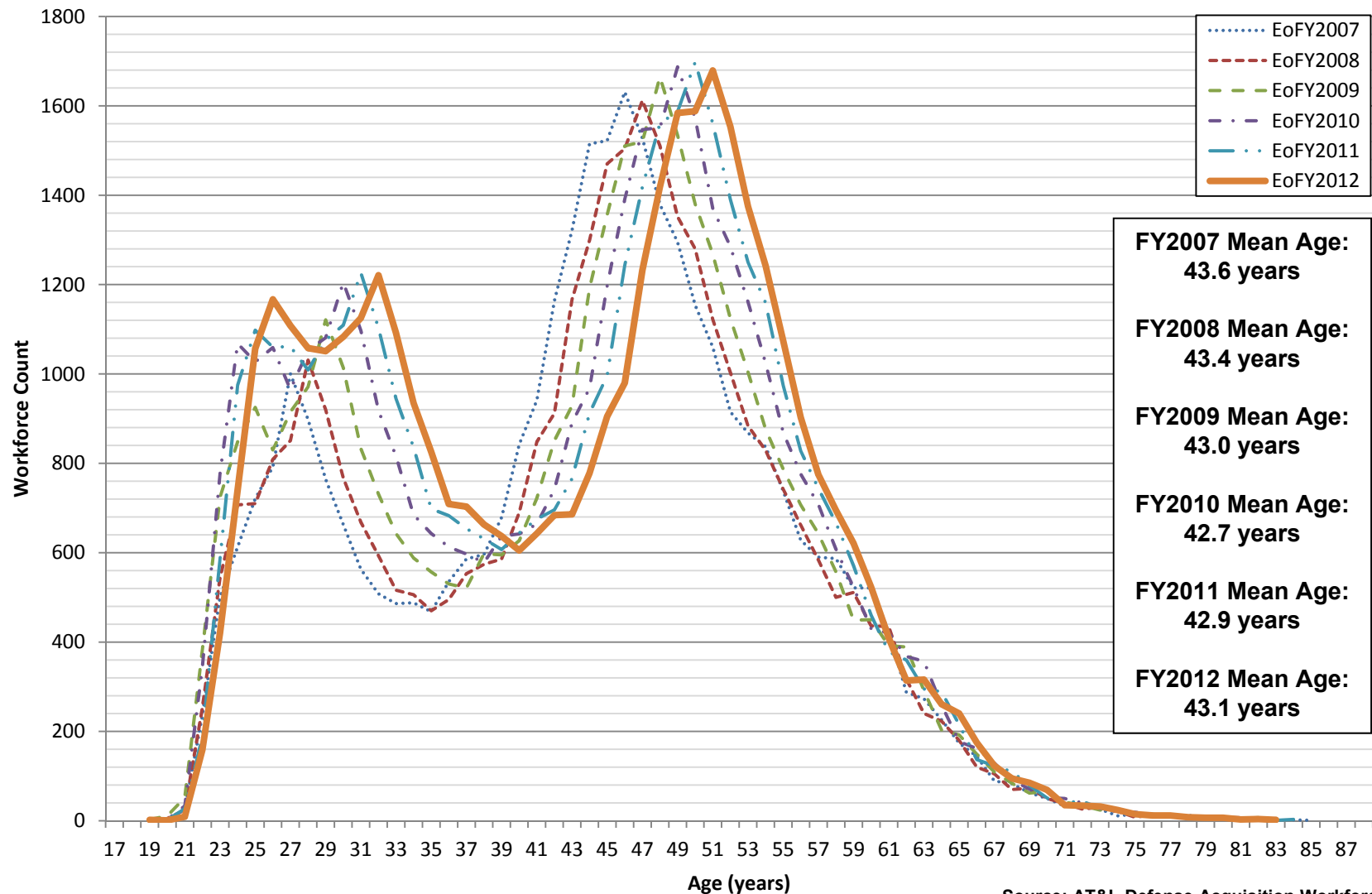
- USD(AT&L), in coordination with the DoD CIO... “shall develop and implement a baseline software assurance policy for the entire lifecycle of covered systems. Such policy shall be included as part of the strategy for trusted defense systems of the Department of Defense.”
- ...“(2) require covered systems to identify and prioritize security vulnerabilities and, based on risk, determine appropriate remediation strategies for such security vulnerabilities;”

NDAA: National Defense Authorization Act <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf>





# DoD SPRDE Workforce: Age Demographics

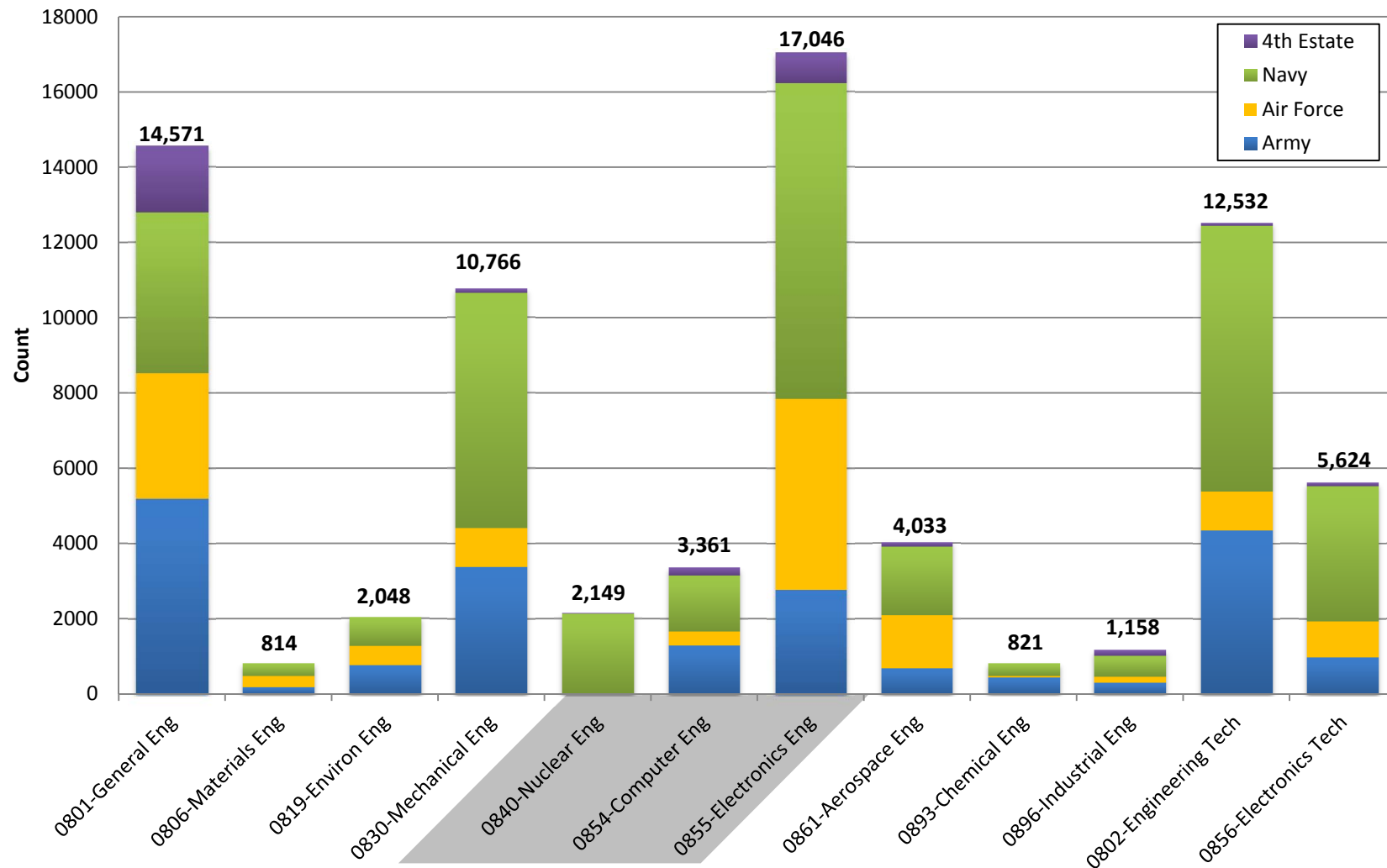


Source: AT&L Defense Acquisition Workforce Data Mart  
SPRDE – Systems Planning, Research, Development and Engineering



# Engineering (Non-Construction) Functional Community by Occupational Series & Component

Total = 74,923



## Notes:

1. 0840, 0854, 0855 designated "Mission Critical Occupations (MCOs)"
2. Does not include 0801A Acquisition Program Management Function

Occupational Series

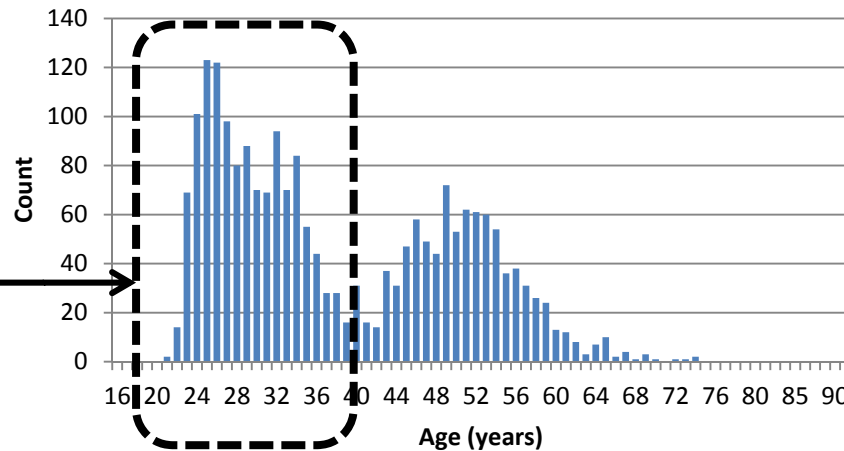
Source: DCPDS, June 30, 2012



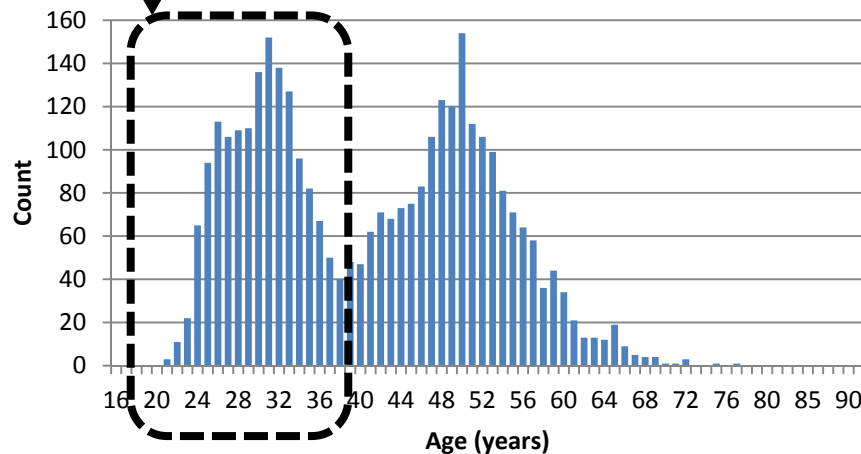
# Mission Critical Occupations: Age by Occupational Series



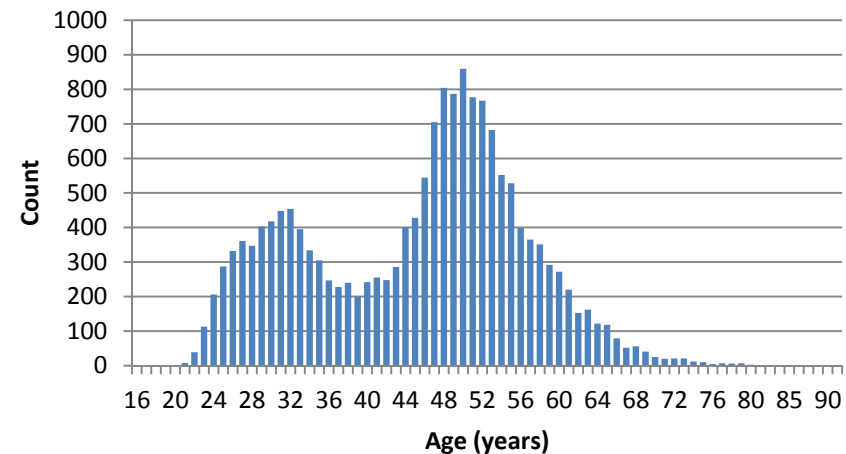
## 0840 - NUCLEAR ENGINEERING



## 0854 - COMPUTER ENGINEERING



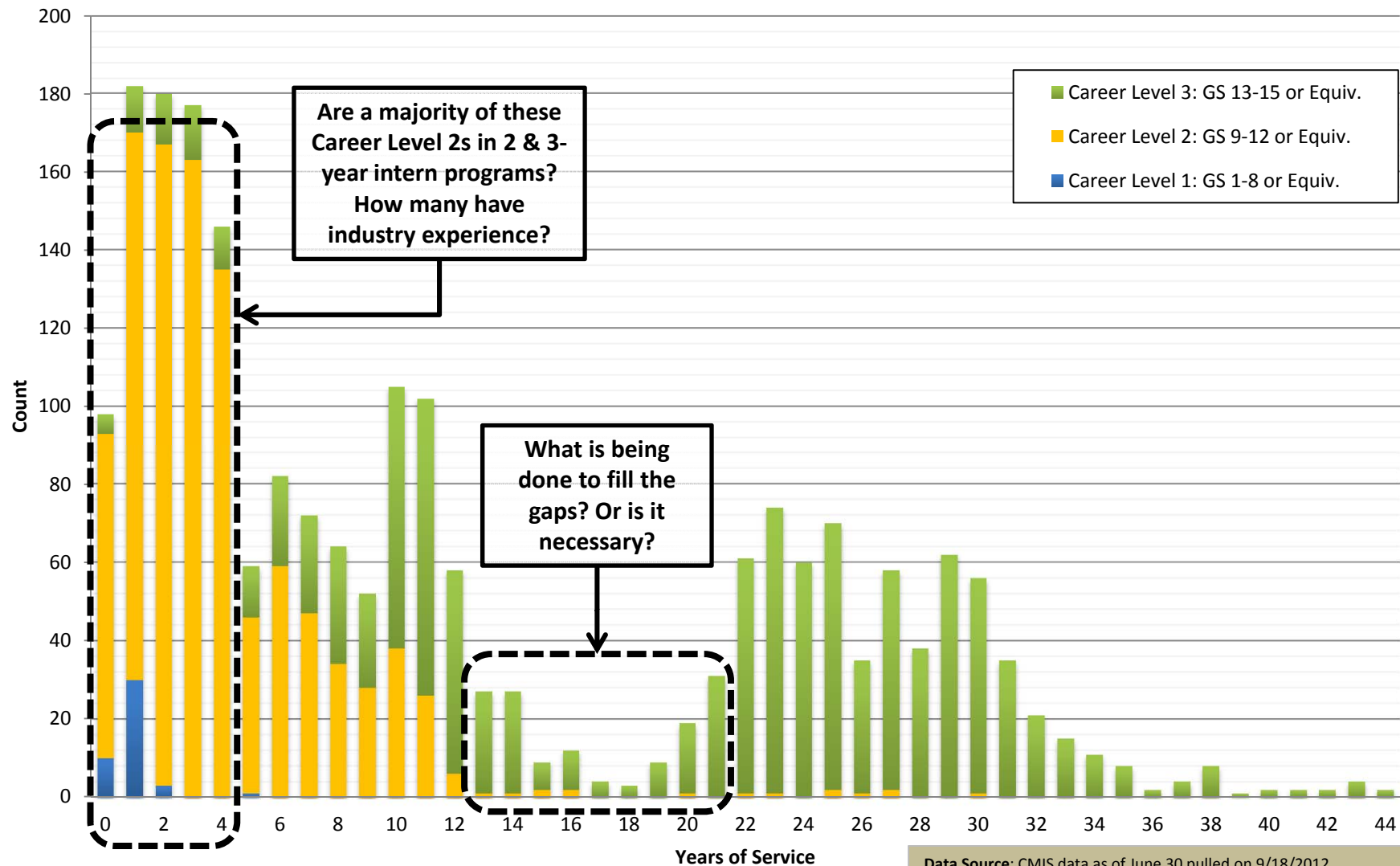
## 0855 - ELECTRONICS ENGINEERING



Source: DCPDS via DRS, June 30, 2012



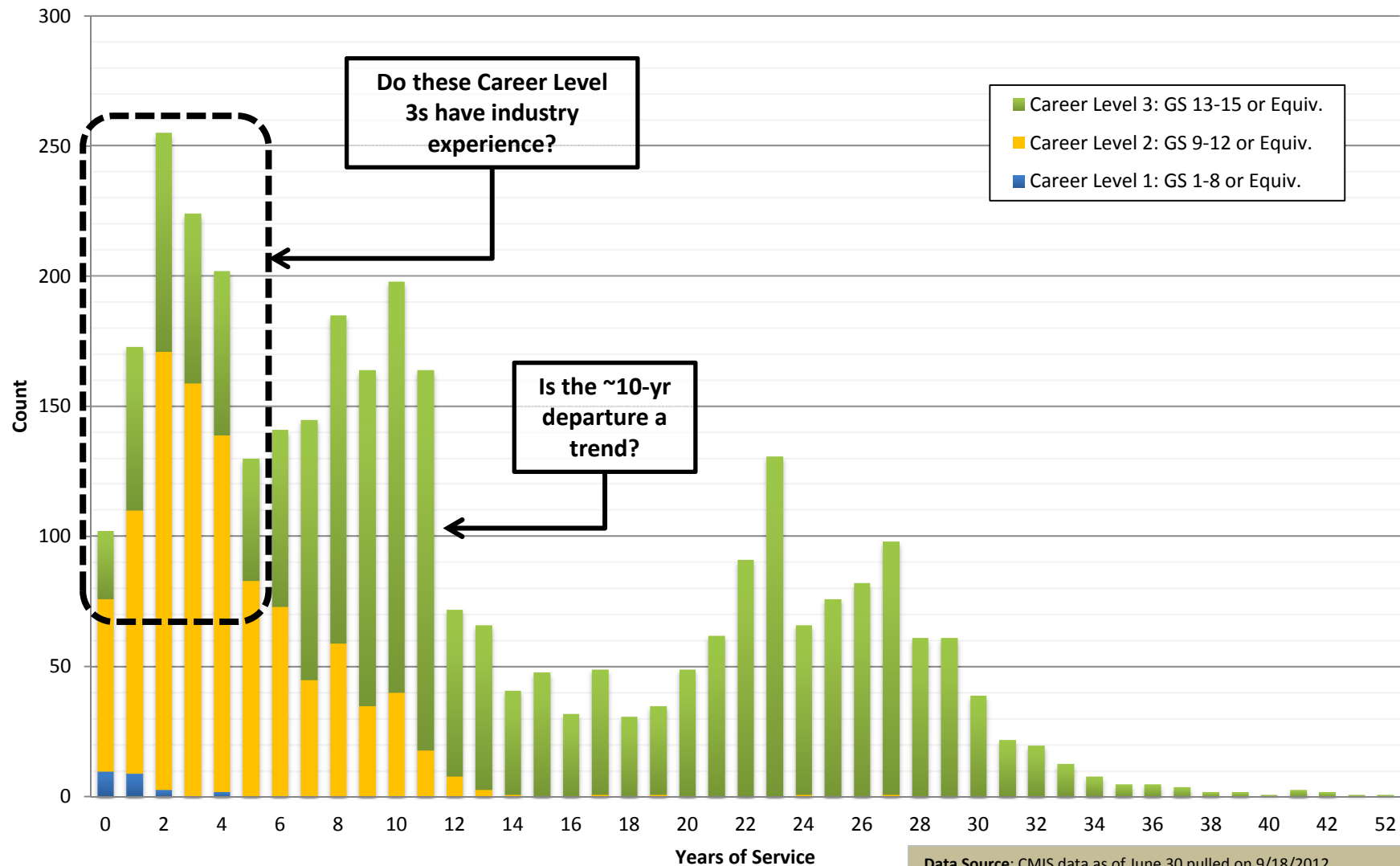
# 0840 – Nuclear Engineers Career Level by Years of Service



Data Source: CMIS data as of June 30 pulled on 9/18/2012  
Population: Appropriated Fund excluding employees in SES like pay plans



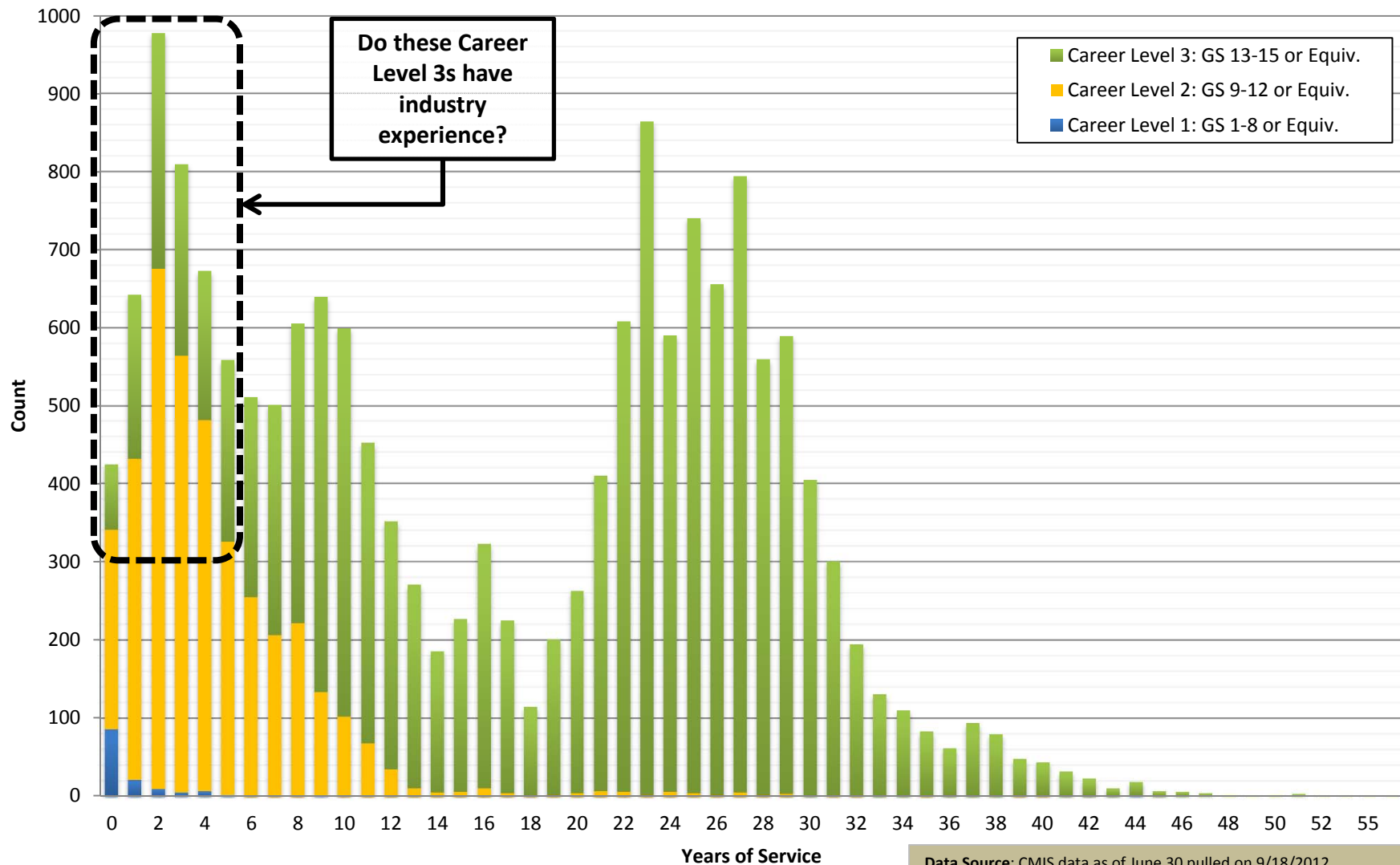
# 0854 – Computer Engineer Career Level by Years of Service



**Data Source:** CMIS data as of June 30 pulled on 9/18/2012  
**Population:** Appropriated Fund excluding employees in SES like pay plans



# 0855 – Electronics Engineer Career Level by Years of Service



Data Source: CMIS data as of June 30 pulled on 9/18/2012  
Population: Appropriated Fund excluding employees in SES like pay plans





# Key Leadership Position Initiative



- **Directed by Sec 820 of PL 109-364 that requires “properly qualified” individuals in key positions on major defense acquisition programs**
- **Further implementation in USD(AT&L)’s 25 Aug 2010 memo, Government Performance of Critical Acquisition Functions**
  - Identifies Program Lead Systems Engineer as a mandatory Key Leadership Position for all MDAP/MAIS programs (Acquisition Categories I and IA) when the function is required based on the phase or type of acquisition program
- **Working with SPRDE FIPT on updating Systems Engineering competencies and determining Key Leadership Position characteristics**

FIPT – Functional IPT

KLP – Key Leadership Position

SPRDE – Systems Planning, Research, Development and Engineering



# Growing Great Engineers

- **Breadth**

- Awareness of and appreciation for other functional areas
- Understanding of system lifecycle and processes
- Knowledge of other engineering disciplines and how they integrate into a system solution
- Knowledge of product domains

- **Depth**

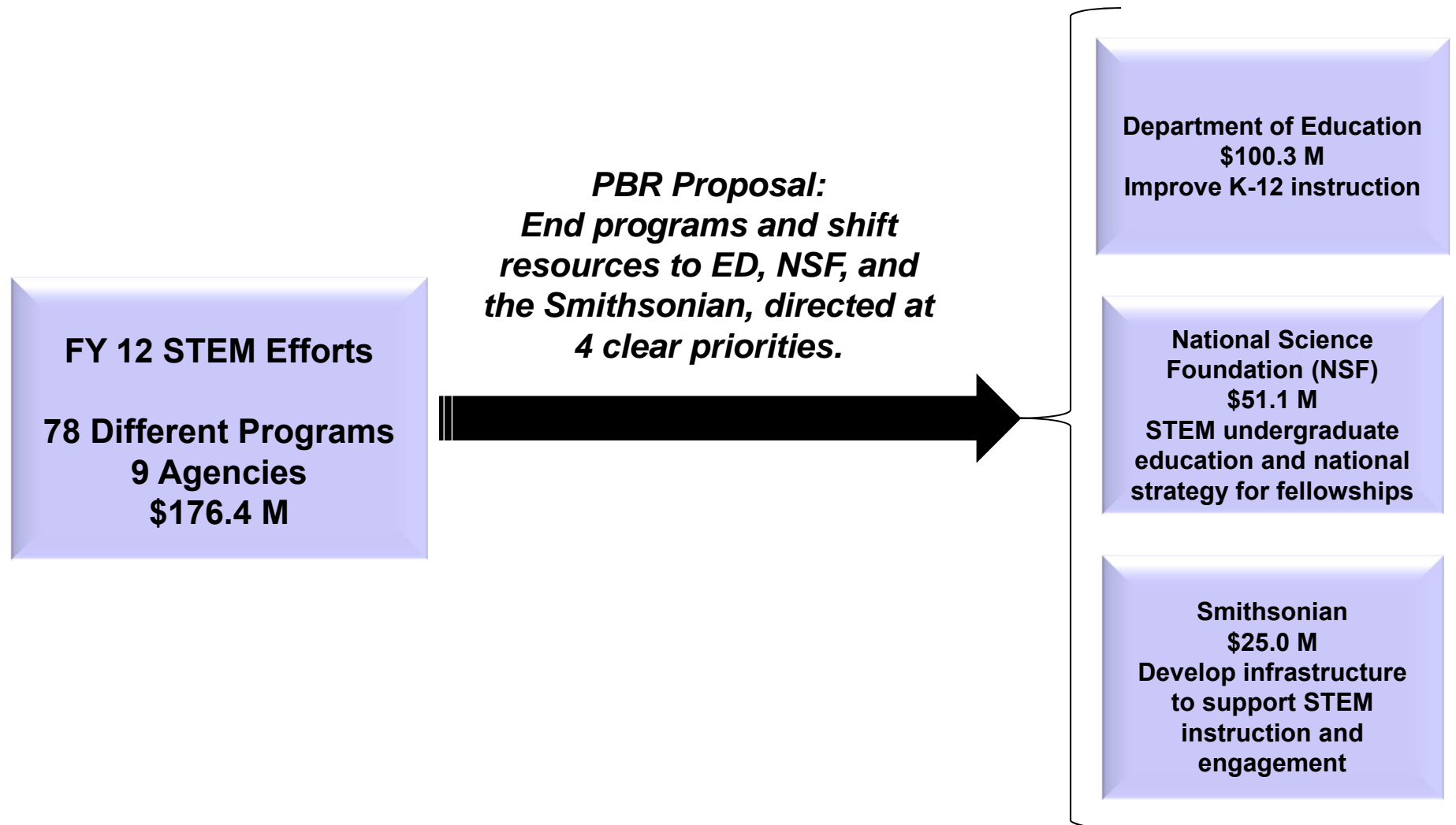
- Extensive expertise and experience in one or more engineering disciplines and in one or more product domains

- **Leadership**

- Ability to motivate and inspire individuals and teams
- Comfort in dealing with complexity
- Focus on underpinning decisions with data
- Capability to make tough technical decisions



# President's Budget Request (PBR) 14 Impact on Federal STEM Education Programs





# FY12 National Defense Authorization Act Sec. 862 Language



## **SEC. 862. ENCOURAGEMENT OF CONTRACTOR SCIENCE, TECHNOLOGY, ENGINEERING, AND MATH (STEM) PROGRAMS.**

***(a) IN GENERAL.—The Under Secretary of Defense for Acquisition, Technology, and Logistics shall develop programs and incentives to ensure that Department of Defense contractors take appropriate steps to--***

- (1) enhance undergraduate, graduate, and doctoral programs in science, technology, engineering and math (in this section referred to as “STEM” disciplines);*
- (2) make investments, such as programing and curriculum development, in STEM programs within elementary and secondary schools;*
- (3) encourage employees to volunteer in Title I schools in order to enhance STEM education programs;*
- (4) make personnel available to advise and assist faculty at such colleges and universities in the performance of STEM research and disciplines critical to the functions of the Department of Defense;*
- (5) establish partnerships between the offeror and historically Black colleges and universities and minority institutions for the purpose of training students in scientific disciplines; or*
- (6) award scholarships and fellowships, and establish cooperative work-education programs in scientific disciplines; or*
- (7) conduct recruitment activities at historically black colleges and universities and other minority-serving institutions or offer internships or apprenticeships.*

***(b) IMPLEMENTATION.—Not later than 270 days after the date of the enactment of this Act, the Under Secretary shall submit to the congressional defense committees a report on the steps taken to implement the requirements of this section.***



# Summary

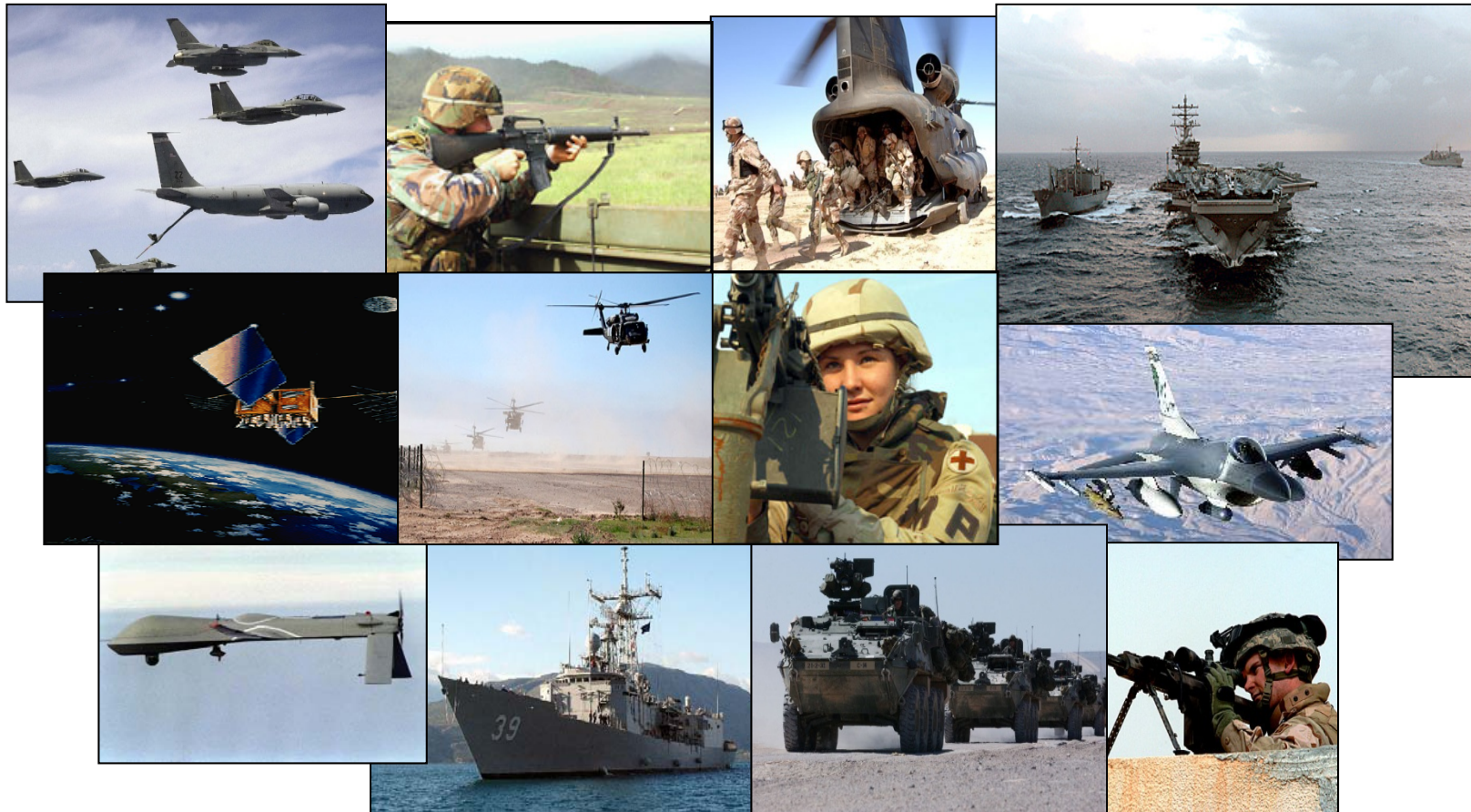


- **FY13 continues to be shaped by budget uncertainty**
- **Criticality of our Systems Engineering mission work has grown**
  - Our work will be even more essential in facing budget challenges
- **We are making an impact**
  - Strong support for System Engineering mission across the Department
- **Dedicated, professional and committed SE staff**
- **Focused on working smarter, as a more tightly integrated team across OSD and the Services**
  - Continue to make a difference for the warfighter and the taxpayer





# Systems Engineering: Critical to Acquisition Success



***Innovation, Speed, and Agility***  
***<http://www.acq.osd.mil/se>***